U.S. Department of Justice
FY 2021 PERFORMANCE BUDGET

Office of the Inspector General

Congressional Justification

Table of Contents

I. Overview (Office of the Inspector General)

Introduction

In Fiscal Year (FY) 2021, the President's budget request for the Department of Justice (DOJ) Office of the Inspector General (OIG) totals $107.2 million, 451 FTE, and 491 positions (143 Agents and 35 Attorneys) to investigate allegations of fraud, waste, abuse, and misconduct by DOJ employees, contractors, and grantees and to promote economy and efficiency in Department operations.

Inspector General's Comments:

The *Inspector General Act* (IG Act) requires me to submit a separate message to Congress when "the Inspector General concludes that the budget submitted by the President would substantially inhibit the Inspector General from performing the duties of the office." (Section 6(f)(3)(E)). The IG Act also requires me to inform Congress of the budget estimate we independently proposed. (Section 6(f)(3)(A)).

The OIG is seeking an additional $3.354 million in its FY 2021 budget request to reflect the difference between the FY 2020 President's Budget Request ($101.646 million) that was used as the baseline for the request and the OIG's FY 2020 enacted funding of $105 million. Without this additional funding, the OIG will not be able to fully implement the proposed IT modernization program enhancement, which is supported by both the Department and the Office of Management and Budget (OMB). When the enacted baseline for the FY 2020 budget ($105 million) and the program increase for IT Modernization ($5.26 million) are factored in, our revised overall request level for FY 2021 is $110.565 million.

Without this level of funding, the OIG's ability to update its aging IT infrastructure and expand its classified computing environment will be limited. The expansion of our classified computing environment is needed to meet the demands of our increased national security workload. For example, as a result of our recent reviews, such as the *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation*, the OIG has been asked and has independently identified the need to increase its oversight of the Department's national security-related programs and operations.

Thank you for considering these comments and for your consistent and strong support for the important mission of the OIG. The DOJ OIG's oversight findings regarding waste, fraud, and mismanagement, our investigative recoveries and our recommendations to more efficiently and effectively manage critical DOJ operations, such as its national security responsibilities, demonstrate the significant and ongoing return on investment in the OIG. We therefore respectfully ask that the Congress fund the OIG at a level of $110.565 million in FY 2021.

Background

The OIG was statutorily established in the Department on April 14, 1989. The OIG is an independent entity within the Department that reports to both the Attorney General and the Congress on issues that affect the Department's personnel or operations.

The OIG has jurisdiction over all complaints of misconduct against DOJ employees, including the Federal Bureau of Investigation (FBI); the Drug Enforcement Administration (DEA); the Federal Bureau of Prisons (BOP); the U.S. Marshals Service (USMS); the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the U.S. Attorneys' Offices (USAO); the Office of Justice Programs (OJP); and other Offices, Boards and Divisions. The one exception is that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorneys' authority to investigate, litigate, or provide legal advice are the responsibility of the Department's Office of Professional Responsibility (OPR).

The OIG investigates alleged violations of criminal and civil law, regulations, and ethical standards arising from the conduct of Department employees in their numerous and diverse activities. The OIG also audits and inspects Department programs and assists management in promoting integrity, economy, efficiency, and efficacy. The Appendix contains a table that provides statistics on the most recent semiannual reporting period. These statistics highlight the OIG's ongoing efforts to conduct wide-ranging oversight of Department programs and operations.

OIG Organization

The OIG consists of the Immediate Office of the Inspector General and the following six divisions and one office:

Audit Division is responsible for independent audits of Department programs, computer systems, and financial statements. The Audit Division has regional offices in Atlanta, Chicago, Denver, Philadelphia, San Francisco, and Washington, D.C. Its Financial Statement Audit Office, Computer Security and Information Technology Audit Office, and Office of Data Analytics are located in Washington, D.C. Audit Headquarters consists of the immediate office of the Assistant Inspector General for Audit, Office of Operations, and Office of Policy and Planning.

Investigations Division is responsible for investigating allegations of bribery, fraud, abuse, civil rights violations, and violations of other criminal laws and administrative procedures governing Department employees, contractors, and grantees. The Investigations Division has field offices in Chicago, Dallas, Denver, Los Angeles, Miami, New York, and Washington, D.C. The Fraud Detection Office and the Cyber Investigations Office are located in Washington, D.C. The Investigations Division has smaller area offices in Atlanta, Boston, Trenton, Detroit, El Paso, Houston, San Francisco, and Tucson. Investigations Headquarters in Washington, D.C. consists of the immediate office of the Assistant Inspector General for Investigations and the following branches: Operations, Operations II, Investigative Support, and Administrative Support.

Evaluation and Inspections Division conducts program and management reviews that involve on-site inspection, statistical analysis, and other techniques to review Department programs and activities and makes recommendations for improvement.

Oversight and Review Division blends the skills of attorneys, investigators, program analysts, and paralegals to review Department programs and investigate sensitive allegations involving Department employees and operations, and manage the whistleblower program.

The Information Technology Division executes the OIG's IT strategic vision and goals by directing technology and business process integration, network administration, implementation of computer hardware and software, cybersecurity, applications development, programming services, policy formulation, and other mission-support activities.

Management and Planning Division provides advice to OIG senior leadership on administrative and fiscal policy and assists OIG components in the areas of budget formulation and execution, security, personnel, training, travel, procurement, property management, telecommunications, records management, quality assurance, internal controls, and general support.

Office of the General Counsel provides legal advice to the OIG management and staff. It also drafts memoranda on issues of law; prepares administrative subpoenas; represents the OIG in personnel, contractual, ethics, and legal matters; and responds to *Freedom of Information Act* requests.

Notable Highlights, Reviews and Recent Accomplishments

1. Managing a Safe, Secure, and Humane Prison System

Maintaining the safety and security of federal inmates and prison employees remains the overriding challenge for the Federal Bureau of Prisons (BOP). However, the specific aspects of that challenge have evolved. For about 20 years, the BOP was managing operations during a period when the inmate population was consistently and substantially increasing. The total federal prison population was about 40,000 in 1985 and it grew to about 220,000 at its peak in 2013, a roughly 450 percent increase. During that period, the BOP faced significant overcrowding across its institutions. However, over the last several years, the number of federal inmates has declined to roughly 180,000. As a result, while overcrowding and providing appropriate housing for inmates continues to be a challenge at some institutions, several other important issues continue to merit identification as top management and performance challenges for the BOP. These include challenges related to the physical safety and security of inmates and staff, inmate health and welfare, and aging and deteriorating facilities and equipment.

Review and Inspection of Metropolitan Detention Center Brooklyn Facilities Issues and Related Impacts on Inmates

In September 2019, the OIG released a Review and Inspection of the Metropolitan Detention Center (MDC) in Brooklyn housing approximately 1,700 federal pre-trial inmates and federal inmates serving sentences. The review consisted of three parts: (1) whether the BOP took appropriate steps to address issues caused by the fire and power outage; (2) how those issues affected the conditions of confinement; and (3) whether the BOP had in place adequate contingency plans to respond to such an incident.

An incident occurred on January 27, 2019, when an electrical fire occurred in the West Building of the MDC causing a partial power outage. The partial power outage wasn't repaired until February 3, 2019, a week later, affecting institutional systems and equipment along with lighting, computers, and phones. During the 7 day power outage, Brooklyn had extreme cold weather for 6 days, with temperatures as low as 2 degrees on January 31st.

The OIG determined there was in fact a heating issue at MDC Brooklyn, but it had nothing to do with the fire or power outage that occurred on January 27th. The OIG found that while the MDC Brooklyn and BOP management did what was needed to insure the safety and security of the facility, they failed many other areas causing inmates to be exposed to 59 degree temperatures, and exceeding 80 degree temperatures. The OIG made 9 recommendations ensuring the BOP is better able to minimize the effect of future failures. The BOP agreed with all 9 recommendations.

__Ongoing Work:__

BOP's Efforts to Address Inmate Sexual Harassment and Sexual Assault against BOP Staff
As of January 2020, the OIG continues to conduct a review of the BOP's efforts to address inmate-on-staff sexual misconduct. The review will assess the prevalence and impacts of inmate-on-staff sexual misconduct, including sexual harassment, assault, and abuse, in BOP institutions from FY 2008 through FY 2018.

Audit of DOJ's Efforts to Protect BOP Facilities against Threats Posed by Unmanned Aircraft Systems
As of January 2020, the OIG continues to audit the Department's efforts to protect BOP facilities against threats posed by unmanned aircraft systems, commonly referred to as drones. The preliminary objectives are to: (1) determine the extent to which the BOP can detect and track attempts to deliver contraband to BOP facilities via drones, and (2) assess the Department's current policies and efforts to protect BOP facilities against security threats posed by drones.

2. Safeguarding National Security and Countering Domestic and International Terrorism

Enhancing national security and countering terrorism remain top priorities for the Department. In FY 2019, the FBI received $5.5 billion to prevent, disrupt, and defeat terrorist operations, prevent and neutralize weapons of mass destruction threats, address cyber threat actors, coordinate counterintelligence activities, facilitate the rapid response to crisis events, and collect intelligence to understand national security and criminal threats. As national security threats continuously change and evolve, so, too, must the Department's approach to combatting those threats. National Security issues relating to Cybersecurity and the Management of Sensitive Investigative Authorities are discussed in separate challenges below.

USA PATRIOT Act, Section 1001
Section 1001 of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT Act) directs the OIG to receive and review complaints of civil rights and civil liberty violations by DOJ employees, to publicize how people can contact the OIG to file a complaint, and to send a semiannual report to the Congress discussing the OIG's implementation of these responsibilities.

Report to Congress on Implementation of Section 1001 of the USA Patriot Act
In August, 2019, the OIG issued its most recent report, summarizing the OIG's Section 1001 activities from January 1, 2019 through June 30, 2019. The report described the number of complaints the OIG received under this section, the status of investigations conducted by the

OIG and the DOJ components in response to those complaints, and an estimate of the OIG's expenses for conducting these activities.

During this period, the OIG processed 441 new civil rights or civil liberties complaints. Of the 441 complaints, 427 complaints did not fall within the OIG's jurisdiction or did not warrant further investigation. Of the 427 complaints, 403 were outside the DOJ so not warranting further review. The OIG determined that the remaining 14 complaints involved DOJ employees or DOJ components and included allegations that required further review. It was determined that all 14 complaints raised management issues, not within the OIG's Section 1001 duties.

Other Activities' Related to Potential Civil Rights and Civil Liberties Issues:
The OIG conducts other reviews that go beyond the explicit requirements of Section 1001 in order to implement more fully its civil rights and civil liberties oversight responsibilities. The OIG completed one such review during the period covered by this report. During this reporting period, the OIG spent approximately $99,577 in personnel costs and $100 in miscellaneous costs, for a total of $99,677 to implement its responsibilities under Section 1001. The total personnel and miscellaneous costs reflect the time and funds spent by OIG Special Agents, Attorneys, Auditors, Inspectors, Program Analysts, and Paralegals who have worked directly on investigating Section 1001-related complaints, conducting special reviews, implementing the OIG's responsibilities under Section 1001, and overseeing such activities.

Disrupting and Defeating Terrorist Threats
In FY 2019, the FBI saw an increase in the threat posed by domestic terrorists, which the FBI defines as individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as political, religious, social, racial, or environmental issues. As required by the Attorney General's Guidelines applicable to FBI Domestic Operations, and as the OIG has long noted, the FBI cannot and must not initiate investigations or collect or maintain information based solely on activities protected by the First Amendment. However, in both the international terrorism and the domestic terrorism realms, distinguishing between First Amendment-protected speech and criminal activity may be particularly difficult in the context of online content or social media posts promoting violence or terrorism.

3. Protecting the Nation and the Department against Cyber-Related Threats

The Department will be challenged to sustain a focused, well-coordinated cybersecurity approach for the foreseeable future. Cybersecurity is a high risk area across the federal government and the Department must continue to emphasize protection of its own data and computer systems, while marshalling the necessary resources to combat cybercrime and effectively engaging the private sector.

For example, the OIG Cyber Investigations Office (Cyber) is currently investigating an international fraud scheme where the subjects are impersonating current DOJ procurement officials and senior leaders to submit fraudulent purchase orders to domestic businesses. Believing these are legitimate purchase orders from the DOJ, the businesses ship laptops, overhead projectors and other IT products to storage locations in the U.S. where it is collected by a co-conspirator and shipped overseas.

Insider Threat Prevention and Detection Program

The Insider Threat Prevention and Detection Program (ITPDP) is designed to deter, detect, and mitigate insider threats from DOJ employees and contractors who would use their authorized access to do harm to the security of the U.S., which can include damage through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities.

There are two parts to the OIG's role in the DOJ ITPDP. One is compliance with DOJ Order 0901 that requires the OIG to work with the Department in its efforts to monitor user network activity relating to classified material and networks. The reporting, training, and coordination requirements in this first role are being implemented by Management & Planning Division's Office of Security Programs. The second part of the ITPDP involves the OIG's Cyber office, which has representatives who act as law enforcement liaisons to the ITPDP relating to Insider Threat referrals. Cyber Special Agents are currently conducting a high profile Insider Threat investigation, which involves international companies and highly sensitive matters. This investigation alone has resulted in the guilty plea of a former DOJ employee and the seizure of over $73 million.

Federal Information Security Modernization Act Audits

The Federal Information Security Modernization Act (FISMA) requires the Inspector General for each agency to perform an annual independent evaluation of the agency's information security programs and practices. Each evaluation includes: (1) testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems; (2) an assessment (based on the results of the testing) of compliance with FISMA; and (3) separate representations, as appropriate, regarding information security related to national security systems.

The OMB is responsible for the submission of the annual FISMA report to the Congress. The Department of Homeland Security (DHS) prepares the FISMA metrics and provides reporting instructions to agency Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy. The evaluation includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. The FY 2019 FISMA results were submitted to OMB on October 31, 2019. The OIG reviewed compliance at six DOJ components: the FBI, JMD, United States National Central Bureau, OJP, Tax Division, and BOP.

Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process

In March 2019, the OIG released an audit report where they examined the FBI's adherence to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, and the FBI Cyber Division Policy Guide 0853 as well as other related policies.

The FBI established Cyber Guardian for tracking the production, dissemination, and disposition of cyber-victim notifications. However, the audit revealed that the data in Cyber Guardian was incomplete and unreliable, making the FBI unable to determine whether all victims are being notified. Additionally, DHS – a partner in using Cyber Guardian – was not entering information into the system as required, contributing to the incompleteness of data in Cyber Guardian. Also, victims identified in cases were not informed of their rights as required by the Attorney General Guidelines for Victim and Witness Assistance. Due to the findings of data being incomplete and unreliable, the FBI plans to replace Cyber Guardian with Cynergy Professional Systems, LLC in

FY 2019. Cynergy Professional Systems, LLC has more than 35 years of experience in mission-critical information technology and communications products and services. They specialize in enterprise networking, WiFi, voice, data, and land mobile radio technology, just to mention a few of their specialties.

The report contains 13 recommendations to assist the FBI and DOJ in improving the efficiency and effectiveness of the cyber victim notification process. Both the FBI and the DOJ fully concurred with the 13 recommendations from the OIG.

Digital Forensics and Cyber Crime Investigations

The OIG's Cyber office continues to conduct computer forensic examinations and mobile device forensic examinations for over 300 pieces of digital evidence annually, which includes computers, hard drives, cell phones, tablets and other electronic media. These examinations support over 100 OIG investigations each year. Cyber reviews numerous referrals from the Justice Security Operations Center (JSOC) regarding the leak or spillage of Personally Identifiable Information and other sensitive DOJ data, to include insider threat allegations, in order to make appropriate disposition in consultation with Investigations Division senior officials. Cyber Special Agents continue to investigate cyber-crime and insider threat matters, as well as attempted intrusions into the Department's network, spoofing of Department emails to accomplish criminal activity, and impersonation of Department officials in furtherance of fraud schemes.

Assessment of and Joint Report on the Implementation of the Cybersecurity Information Sharing Act (CISA) of 2015

On December 18, 2015, the Congress passed Public Law 114-113, the Consolidated Appropriations Act, 2016, which includes Title I – the Cybersecurity Information Sharing Act of 2015 (the Statute). The Statute was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information. The Statute creates a framework to facilitate and promote the voluntary sharing of cyber threat indicators and defensive measures among and between Federal and non-Federal entities.

On December 18, 2019, a Joint Assessment and Report was submitted to the Congress regarding the actions taken in carrying out the CISA requirement during 2017 and 2018. The Inspectors General of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, and the Intelligence Community assessed the actions taken over the prior, most recent, two-year period to carry out the requirements of CISA.

The report determined that sharing of cyber threat indicators and defensive measures within the intelligence community has improved over the past two years, and efforts are underway to expand accessibility to information, but sharing by the private sector using the automated indicator sharing capability remains a challenge.

Ongoing Work:

FBI's Strategy and Efforts to Disrupt Illegal Dark Web Activities

As of January 2020, the OIG is auditing the FBI's strategy and efforts to disrupt illegal dark web activities. The preliminary objective is to assess the implementation of the FBI's dark web strategy.

4. Management of Sensitive Investigative Authorities

The Department is empowered to use certain sensitive investigative tools, such as confidential sources, bulk data collection, and conducting surveillance pursuant to a court order under the Foreign Intelligence Surveillance Act (FISA). These tools pose risks if they are employed without adequate management and oversight. Recent and past OIG reviews have found that the Department faces challenges in using these sensitive authorities consistent with its policies, and in a manner that safeguards individuals' statutory and constitutional privacy rights. The actual or perceived misuse of such authorities can undermine the public's trust and confidence in the Department, impact the Department's standing with the judiciary, threaten the success of prosecutions, and lead to the amendment or revocation of certain authorities.

Review of Four Foreign Intelligence Surveillance Act (FISA) Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

On December 9, 2019, the OIG released a report examining, among other things, the decision to open the Crossfire Hurricane counterintelligence investigation, and four individual cases on current and former members of the Trump presidential campaign; the FBI's relationship with Christopher Steele, whom the FBI considered to be a confidential human source (CHS); four FBI applications filed with the Foreign Intelligence Surveillance Court (FISC) in 2016 and 2017 to conduct FISA surveillance targeting Carter Page; the interactions of DOJ attorney Bruce Ohr with Steele, the FBI and others as they related to the investigation; and the FBI's use of undercover employees (UCEs) and CHSs other than Steele in the investigation. In the report, the OIG made several significant findings, including that:

- The opening of the Crossfire Hurricane investigation was in compliance with Department and FBI policies, and we did not find documentary or testimonial evidence that political bias or improper motivation influenced the decision to open the investigation;

- Department and FBI policies do not require Department consultation before opening an investigation involving the alleged conduct of individuals associated with a presidential campaign;

- The CHS operations that the Crossfire Hurricane team undertook were approved, as required, under FBI policy and were permitted under Department and FBI policy;

- Department and FBI policies do not require the FBI to consult with any Department official in advance of conducting CHS operations involving advisors to a presidential campaign, and we found no evidence that the FBI consulted with any Department officials before conducting these CHS operations; and

- There were inaccuracies and omissions in the FISA applications that resulted from case agents providing wrong or incomplete information to Department attorneys. We identified significant inaccuracies and omissions in each of the four applications: seven in the first FISA application and a total of 17 by the final renewal application.

The OIG made several recommendations to assist the Department and the FBI in addressing the problems identified in the review. In addition, we referred our findings related to: (1) the FBI personnel who had responsibility for the preparation, Woods review, or approval of the FISA applications, as well as the managers, supervisors, and senior officials in the chain of command of the Carter Page investigation; (2) the actions of an FBI attorney who altered documents related to the preparation of the final Carter Page FISA renewal application; and (3) Bruce Ohr's conduct to the relevant entities in the Department and the FBI for appropriate action.

Investigation of Former FBI Director James Comey's Disclosure of Sensitive Investigative Information and Handling of Certain Memoranda

In August 2019, the OIG released a report examining former FBI Director James B. Comey's retention, handling, and dissemination of certain memoranda memorializing seven one-on-one interactions with then President-Elect Donald J. Trump between January 6, 2017, and April 11, 2017.

The OIG concluded that the memos were official FBI records and that Mr. Comey violated applicable policies and his FBI employment agreement by providing one of the unclassified memos that contained FBI information, including sensitive information, to his friend with instructions to share that information with a reporter. Additionally, the OIG determined that Mr. Comey failed to follow FBI policies and his FBI employment agreement by: (1) keeping four of the seven memos in a personal safe at his home and failed to notify the FBI after his removal as FBI Director or request authorization to retain them, (2) after his removal as FBI Director, providing the four memos to his three private attorneys without FBI authorization; and (3) failing to notify the FBI about his disclosures to his private attorneys after learning that the FBI had determined that one of the memos included sensitive information classified at the Confidential level.

Upon completing the investigation, the OIG provided the factual findings to the DOJ for a prosecutorial decision regarding Comey's conduct, as required by the Inspector General Act. After reviewing the matter, the DOJ declined prosecution.

Audit of the Federal Bureau of Investigation's Management of its Confidential Human Source Validation Processes

In November 2019, the OIG released the results of an audit conducted to: (1) evaluate the FBI's Confidential Human Source (CHS) program policies and procedures, including its validation procedures; (2) assess the FBI's policies and procedures for the use of non-attributable communications between agents and CHSs; and (3) examine the FBI's ability to identify and fill gaps in the alignment of its CHSs with the nation's highest priority threats and intelligence needs.

In the end, the OIG found that: (1) the FBI did not comply with the Attorney General's Guidelines for vetting Confidential Human Sources (CHS); (2) there were deficiencies in the FBI's long-term CHS validation reports, which are used in determination of further CHS use; (3) the FBI inadequately staffed and trained personnel conducting long-term validations and lacked an automated process to monitor the CHSs; (4) the Joint DOJ-FBI committee having oversight of the CHS program had a backlog of CHSs waiting for determination of future use, allowing them to potentially operate when they should not have; and (5) the FBI plans to use a proposed system that relies on data from another system with known data quality issues.

The OIG made 16 recommendations to better help the FBI manage its CHS program. The FBI concurred with all 16 recommendations made to the FBI and the Department.

DEA's Use of Administrative Subpoenas
In March 2019, the OIG released a review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data. The DEA is authorized to issue administrative subpoenas, without court or other approval outside the agency, requiring the production of records that are "relevant or material" to certain drug investigations.

The OIG examined three programs (two involving the collection or exploitation of bulk telephone records, and the third involved the collection of bulk purchase transaction data) in which the DEA used its administrative subpoena authority to collect or exploit bulk collections of data. The determination by the OIG found that the DEA (and DOJ with respect to one program) failed to conduct a comprehensive legal analysis of the use of the DEA's administrative subpoena authority to collect or exploit bulk data.

In this report the OIG made 16 recommendations to the DEA and DOJ to address the issues and concerns the OIG identified. The Department and the DEA agreed with all of the recommendations.

Ongoing Work:

FBI's National Security Undercover Operations
As of January 2020, the OIG continues to audit the FBI's National Security Undercover Operations. The preliminary objectives are to evaluate: (1) the FBI's oversight of national security-related undercover operations, and (2) the FBI's efforts to recruit and train agents for these undercover operations.

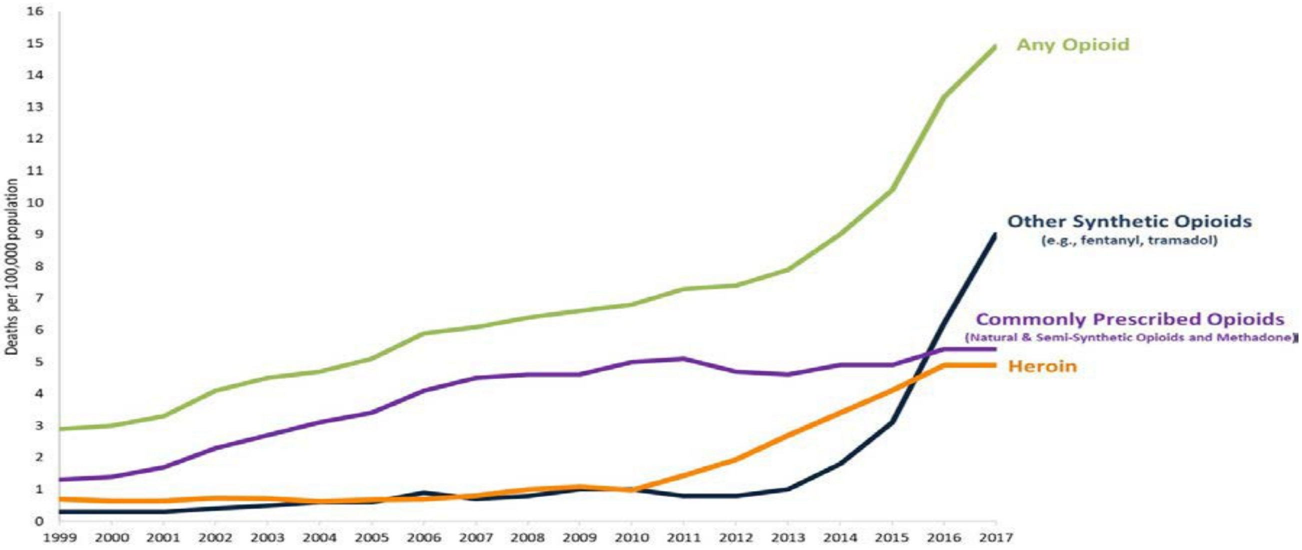
5. Law Enforcement Coordination and Community Engagement

The Department's top law enforcement priorities, which include combatting the opioid crisis, reducing violent crime, and investigating cross-border criminal activity, are most effectively addressed through cooperation among federal agencies, partnerships with state, local, and tribal law enforcement agencies, and engagement with impacted communities. Below, we detail some of the challenges the Department faces in addressing these law enforcement priorities.

Review of the Drug Enforcement Administration's Regulatory and Enforcement Efforts to Control the Diversion of Opioids
In September 2019, the OIG issued a report examining the regulatory activities and enforcement efforts of the DEA from FY 2010 through FY 2017 to combat the diversion of opioids to unauthorized users.

According to the Centers for Disease Control and Prevention (CDC), as of 2017, more than 130 people die every day in the United States from opioid overdose. Since 2000, more than 300,000 Americans have lost their lives to an opioid overdose. The misuse of and addiction to opioids, including prescription pain relievers, heroin, and synthetic opioids such as fentanyl, has led to a national crisis that affects not only public health, but also the social and economic welfare of the country. As a result, in October 2017 the White House declared the opioid epidemic a public health emergency.

Overdose Deaths Involving Opioids, by Type of Opioid, United States 2000-2017



Source: CDC National Vital Statistics System Mortality File

We found that the DEA was slow to respond to the significant increase in the use and diversion of opioids since 2000. We also found that the DEA did not use its available resources, including its data systems and strongest administrative enforcement tools, to detect and regulate diversion effectively. Further, we found that DEA policies and regulations did not adequately hold registrants accountable or prevent the diversion of pharmaceutical opioids. Lastly, we found that while the Department and the DEA have recently taken steps to address the crisis, more work is needed.

The OIG made 9 recommendations to improve the Department's and DEA's ability to combat the diversion of pharmaceutical opioids and effectively target and regulate registrants that engage in diversion. The DEA concurred with the 7 recommendations directed to the DEA.

Audit of Efforts to Safeguard Minors in Department of Justice Youth-Centered Programs

In March 2019, the OIG issued an audit examining the efforts to safeguard minors in DOJ youth-centered programs. The preliminary scope includes the OJP and the Office on Violence Against Women youth-centered FY 2017 grant programs involving persons who work directly with minors. The OIG's preliminary objectives were to: (1) determine whether entities receiving DOJ funds have implemented appropriate controls, such as screening and background checks, for individuals working or volunteering in programs involving minors; and (2) assess DOJ efforts to ensure that grantees adequately mitigate the risk of victimization of minors who participate in its youth-centered programs.

We identified a number of significant issues pertaining to DOJ's lack of consistent policies and procedures to best ensure the safeguarding of minors involved in DOJ grant-funded projects. We found a lack of specific guidance and formal award requirements for grantees regarding background screening of individuals participating in DOJ grant programs who are in direct contact with minors, as well as an absence of a consistent monitoring regime to determine what steps, if any, grantees and subgrantees have taken to screen individuals working closely with children.

Our report contains 6 recommendations to ensure that DOJ grantees have adequate controls in place to safeguard minors participating in DOJ-funded programs, and to ensure that the DOJ takes appropriate steps to monitor this issue and mitigate the risk of victimization of minors in its programs.

6. Administering and Overseeing Contracts and Grants

In FY 2019, the Department obligated over $8.5 billion in contracts and awarded approximately $7.5 billion in grants. Although the Department has made some recent improvements to its administration and oversight of contracts and grants, we identified continued deficiencies in these areas, which present significant fraud and mismanagement risks.

Audit of the Office of Community Oriented Policing Services Tribal Resource Grant Program Awards to the Choctaw Nation of Oklahoma, Durant, Oklahoma

In September 2019, the OIG released an audit report conducted with two purposes; (1) to determine whether costs claimed under the grants were allowable, supported, and within the applicable laws; and (2) to determine whether the grantee's progress toward goal achievement was adequately demonstrated.

The Office of Community Oriented Policing Services (COPS) awarded a total of $3.1 million from five grants to the Choctaw Nation of Oklahoma (CNO).

The OIG concluded that the CNO did in fact demonstrate adequate progress toward achieving their goals, except for one. The CNO failed to purchase the communication equipment needed to fill critical gaps in its communication systems under Grant Number 2014-HE-WX-0044.

The OIG concluded that these deficiencies resulted in $41,063 in unallowable costs and another $60,643 in unsupported costs. After the draft report was issued, the CNO provided documentation that $49,140 was supported, leaving $11,503 as unsupported. The OIG made 13 recommendations to COPS.

Review of the Office of Justice Programs' Efforts to Address Challenges in Administering the Crime Victims Fund Programs

In July 2019, the OIG released a review of OJP's efforts to address challenges in administering Crime Victims Fund (CVF) Programs. In FY 2015, the Congress more than tripled the amount of CVF funds available for distribution by the Department to support victims from $750 million to nearly $2.4 billion, and by FY 2018, the program totaled over $4.4 billion.

The OIG has received $10 million from the CVF each year since 2015 to conduct oversight of the Department's awards for victims and victim services. As a result, the OIG has conducted numerous audits of CVF grant recipients. The OJP awards the bulk of CVF grant funds to states and territories. We have observed several recurring issues that warrant the Department's attention to ensure proper administration and oversight of this substantial grant award program.

The OIG has issued nearly 50 CVF-related audits in 2016, focused primarily on state programs and how the OJP administers the CVF grants to states individually. This review also assessed systemic issues with grant administration as well as evaluated how the OJP addressed programmatic issues that were identified in previous audits.

The OIG found that the OJP has worked very hard helping states achieve the objectives of the CVF grant programs and addressing rising challenges. At the same time several ways were identified that fell short of the objectives, and there is also concern that shortcomings within OJP's oversight may be intensified in an area where the CVF funding has significantly increased and there's been a reduction in staffing. Based on the results of the review, the OIG made 14 recommendations to improve OJP's administration of the CVF programs.

Audit of the Federal Bureau of Investigation's Oversight and Administration of the National Vehicle Lease Program and Its Contract with EAN Holdings, LLC

In March 2019, the OIG released an audit report assessing the FBI's administration of the EAN Holdings, LLC contract, and EAN's (also known as Enterprise Rent-A-Car) performance and compliance with the terms, conditions, and regulations applicable to this contract. Also, the OIG examined the FBI's implementation of the National Vehicle Lease Program (NVLP), which this contract directly supports.

Overall, Task Force Officers were generally satisfied with the vehicles provided by EAN; however, operational concerns were discovered associated with the FBI's decision to transition from EAN vehicles to exclusively General Services Administration vehicles. We identified deficiencies with the FBI's administration, oversight, and monitoring of its EAN contract. The OIG found the FBI's review of invoices was not adequate, resulting in $538,791 in questioned costs and nearly $1 million in fuel purchases that do not appear to be permitted under NVLP guidelines.

The OIG made 21 recommendations to assist the FBI in improving its implementation of the NVLP and its contract administration, oversight, and monitoring. The FBI concurred with all of the OIG's recommendations.

Audit of the Federal Bureau of Prison's Perimeter Security Upgrade Contract for Administrative U.S. Penitentiary Thompson Awarded to DeTekion Security Systems, Incorporated

In March 2019, the OIG completed an audit of the Firm Fixed Price contract between the BOP and DeTekion Security Systems, Incorporated (DeTekion) totaling $2.4 million. DeTekion was contracted to construct an electronic taut wire fence detection system at Administrative U.S. Penitentiary Thompson, in Thompson, IL. The OIG found that the BOP did not comply with the Federal Acquisition Regulation (FAR), raising concerns that the BOP's process for awarding this contract were flawed.

The BOP limited competition, awarding a sole source contract knowing that there were other companies that may be able to do the same type of fence, resulting in no assurance that the BOP obtained the most advantageous bid. The OIG's report contains 9 recommendations aiding the BOP in improving its contracting practices. The BOP agreed with all of the OIG recommendations.

<u>Ongoing Work:</u>

Audit of Contracts Awarded for Covert Contracts

As of January 2020, the OIG continues to audit the FBI's contracts awarded for covert activity. The preliminary objectives of the audit are to: (1) assess the FBI's awarding and administration of these covert contracts, and (2) evaluate the FBI's procedures and processes for ensuring contractor performance and compliance with the terms, conditions, laws, and regulations applicable to these contracts.

7. Using Performance-Based Management

Performance-based management has been a long-standing challenge not only for the Department but across the entire federal government. OMB Circular No. A-11 and the *Government Performance and Results Modernization Act* (GPRA Modernization Act) place a heightened emphasis on priority-setting, cross-organizational collaboration to achieve shared goals, and the use and analysis of goals and measurements to improve outcomes. A significant management challenge for the Department is ensuring, through performance-based management, that its programs are achieving their intended purposes. The OIG will ensure that the Department is effectively implementing performance-based management and taking actions to meet the requirements of the GPRA Modernization Act.

DOJ OIG Issues Procedural Reform Recommendations for the U.S. Marshals Service Concerning the Imposition of Prompt and Effective Discipline for Employee Misconduct

The OIG issued a Procedural Reform Recommendation (PRR) in February 2019 for the USMS. The OIG releases PRRs when, through its investigative work, it finds a systematic weakness in the Department's operations, programs, policies, procedures, or practices, and has a recommendation to address the identified problem.

This PRR was issued in response to a senior-level USMS employee who retired with his full pension without serving any disciplinary penalty, despite two OIG investigations that substantiated allegations of serious misconduct by the senior employee. It is the OIG's view that prompt disciplinary action in response to substantiated misconduct findings serves several important principles: accountability; deterrence; integrity of the workforce; preservation of resources; and maintaining employee morale.

Accordingly, the PRR recommends that the USMS implement policies, procedures, and internal controls to address deficiencies in its processing of adverse personnel actions that were exposed in the USMS response to these investigations, and ensure prompt and effective imposition of appropriate discipline in cases of substantiated employee misconduct. By statute, this report is required to be included in the DOJ annual Agency Financial Report.

Top Management Challenges

The OIG has published a report on the top management and performance challenges facing DOJ annually since 1998. On November 27, 2019, the OIG published it's most recent list of top management and performance challenges facing DOJ based on the OIG's oversight work, research, and judgment.

This year's report identifies eight challenges that the OIG believes represent the most pressing concerns for the DOJ. While the challenges are not rank-ordered, the OIG believes that challenges in three critical areas—prisons, national security, and cybersecurity—will continue to occupy much of the Department's attention and require vigilance for the foreseeable future.

In addition, the OIG has identified one new challenge, the need for the Department to effectively manage and oversee its exercise of certain sensitive investigative authorities, such as the use of confidential sources and surveillance authorized under the Foreign Intelligence Surveillance Act, as an emerging issue that merits DOJ's continued attention. Meeting all of these challenges will require the DOJ to develop innovative solutions and conduct careful monitoring of its efforts to achieve success.

8. Fostering a Diverse, Highly-Skilled Workforce

The Department faces a number of challenges in its efforts to ensure that it has a diverse, highly-skilled workforce with the expertise necessary to accomplish its mission. These include challenges related to recruiting and retaining employees to fill certain mission critical positions, and to ensuring that the Department's specialized expertise and institutional knowledge is not lost through retirement.

The Department faces challenges in both recruiting and retaining employees in a highly competitive marketplace. The Department's efforts to recruit and retain skilled employees may be hindered by declining employee engagement, work-life balance concerns, and its lack of diversity in certain key positions.

The Department faces challenges in recruiting and retaining employees to fill certain mission critical positions, such as healthcare and cyber-related positions. As noted in previous years' reports, healthcare professionals and cyber-professionals are highly sought after in the private sector and often receive salaries that cannot be matched with the federal pay scale. As a result, the Department must work within existing laws and regulations to provide compensation packages and work-life opportunities to remain competitive with the private sector.

CyberSecurity Workforce
In a March 2019 report, the GAO found that the Department was unable to comply with the requirements of the Federal Cybersecurity Workforce Assessment Act of 2015 to identify filled and vacant positions within IT, cybersecurity, and cyber-related functions. The GAO found that by not completing its efforts to identify its vacant IT, cybersecurity, and cyber-related positions, the Department lacks important information about the state of its workforce. As a result, the Department's ability to identify work roles of critical need and improve workforce planning may be limited.

Federal Employee Viewpoint Survey, Government-wide Report
In its 2019 government-wide report, the Office of Personnel Management (OPM) found that work-life programs have a positive impact on recruitment, retention, performance, and employee morale. In the most recent OPM Federal Employee Viewpoint Survey (FEVS) results, the OIG ranked 22 out of 420 Agency Components in the area of work-life balance. The OIG again received the highest Global Satisfaction Score in the Department, with an increase to 82 percent this year, and also had an Engagement Index Score of 82 percent, as compared to 80 percent and 82 percent, respectively, in 2018. The OIG's New Inclusion Quotient (New IQ) score, which measures the inclusiveness of the work environment based on Five Habits of Inclusion (Fair, Open, Cooperative, Supportive, and Empowering) was 77%, the same as in 2018.

9. Whistleblower Ombudsperson

Whistleblowers perform a critical role when they bring forward evidence of wrongdoing, and they should never suffer reprisal for doing so. The OIG Whistleblower Coordinator Program (the Whistleblower Program) works to ensure that whistleblowers are fully informed of their rights and protections from reprisal.

The DOJ OIG Whistleblower Program continues to play a leadership role in the Council of Inspectors General on Integrity and Efficiency's (CIGIE) efforts to educate and empower whistleblowers to come forward with lawful disclosures of misconduct. In July 2019, the Whistleblower Program helped to coordinate a CIGIE-wide effort to launch a new online tool and resource page for whistleblowers. The online tool allows users to respond to a few simple prompts, and they are then directed to the appropriate Inspector General, the Office of Special Counsel (OSC), or other entity to report wrongdoing or to file a retaliation complaint. CIGIE and OSC launched the tool during its BETA test to provide the public an opportunity to provide feedback before the tool was final. To further guide individuals who want to report waste, fraud, abuse, or retaliation, the site also provides specific information to individuals in various sectors, such as whistleblower protections for contractors and grantees, members of the military services, and intelligence community employees.

In connection with National Whistleblower Appreciation Day, which was July 30, 2019, CIGIE also released a new report to highlight whistleblowers' impact. The report, titled "Whistleblowing Works: How Inspectors General Respond to and Protect Whistleblowers," highlights OIG investigations, audits, and reviews that were initiated or advanced because of a whistleblower disclosure. All of those OIG reports, along with examples of OIG efforts to protect whistleblowers from retaliation, are available on Oversight.gov.

On June 25, 2018, President Trump signed into law *S. 1869, the Whistleblower Protection Coordination Act.* The new law, sponsored by Senator Charles Grassley, renamed the position of OIG Whistleblower Ombudsman to the Whistleblower Protection Coordinator. Importantly, the Act also made the Whistleblower Protection Coordinator a permanent position, a clear indication of the program's success throughout the IG community and the Congress' interest in institutionalizing a whistleblower support and education role within the OIGs.

In addition to renaming and reauthorizing the Coordinator position, the legislation requires CIGIE, in consultation with the Office of Special Counsel and Whistleblower Protection Coordinators, to "develop best practices for coordination and communication in promoting the timely and appropriate handling and consideration of protected disclosures, allegations of reprisal, and general matters regarding the implementation and administration of whistleblower protection laws."

The DOJ OIG also continues to utilize the tracking system developed through the OIG Ombudsperson Program to ensure that it is handling these important matters in a timely manner. The DOJ OIG continuously enhances the content on its public website, oig.justice.gov. The table below, pulled from our *Semiannual Report to Congress, April 1, 2019 - September 30, 2019,* presents important information.

Whistleblower Program
April 1, 2019 – September 30,2019

Employee complaints received[4]	199
Employee complaints opened for investigation by the OIG	64
Employee complaints that were referred by the OIG to the components for investigation	69
Employee complaint cases closed by the OIG[5]	59

The DOJ OIG continues to refine its internal mechanisms to ensure prompt reviews of whistleblower submissions and communication with those who come forward with information in a timely fashion.

10. Congressional Testimony

The Inspector General testified before Congress on the following occasions:

- "Protecting Those Who Blew the Whistle on Government Wrongdoing" before the House Committee on Oversight and Reform on January 20, 2020;

- "DOJ OIG FISA Report: Methodology, Scope, and Findings" before the U.S. Senate Committee on Homeland Security and Governmental Affairs on December 18, 2019;

- "Examining the Inspector General's Report on Alleged Abuses of the Foreign Intelligence Surveillance Act" before the U.S. Senate Committee on the Judiciary on December 11, 2019;

- "Overseeing the Overseers: Council of the Inspectors General on Integrity and Efficiency @ 10 years" before the U.S. House of Representatives Committee on Oversight and Reform on September 18, 2019.

11. Support for the Department’s Savings and Efficiencies Initiatives

In support of DOJ’s $AVE initiatives, the OIG contributed to the Department’s cost-saving efforts in FY 2019, including:

- *Increasing the use of self-service online booking for official travel*. Through December 2019, the OIG’s on-line booking rate for FY 2020 official travel was 94% for a savings of $37,075 over agent assisted ticketing costs. Online reservations cost $9.35 per transaction, compared to $37.63 per agent-assisted transaction.

- *Using non-refundable airfares rather than contract airfares or non-contract refundable fares (under appropriate circumstances)*. Through December 2019 of FY 2020, the OIG realized cost savings of $1,983. Nonrefundable tickets should be considered when the cost is lower than the contract fare, and there is a high degree of certainty that cancellation or changes in travel arrangements will not be necessary. The OIG has the potential to achieve substantial cost savings from non-refundable tickets, so use of non-refundable fares is encouraged as mission permits.

- *Increased use of video conferencing*. The OIG saved training and travel dollars, as well as productive staff time while in travel status, by utilizing increased video teleconferencing for all applicable OIG-wide training.

Getting the most from taxpayer dollars requires ongoing attention and effort. The OIG continues to look for ways to use its precious resources wisely and to examine how it does business to further improve efficiencies and reduce costs.

Challenges

Like other organizations, the OIG must confront a variety of internal and external challenges that affect its work and impede progress towards achievement of its goals. These include decisions made by Department employees while carrying out their numerous and diverse duties, which affect the number of allegations the OIG receives, and financial support from the OMB and the Congress.

The limitation on the OIG’s jurisdiction has also been an ongoing impediment to strong and effective independent oversight over agency operations. While the OIG has jurisdiction to review alleged misconduct by non-lawyers in the Department, it does not have jurisdiction over alleged misconduct committed by Department attorneys when they act in their capacity as lawyers—namely, when they are litigating, investigating, or providing legal advice. In those instances, the IG Act grants exclusive investigative authority to the Department’s OPR office. As a result, these types of misconduct allegations against Department lawyers, including any that may be made against the most senior Department lawyers (including those in departmental leadership positions), are handled differently than those made against agents or other Department employees. The OIG has long questioned this distinction between the treatment of misconduct by attorneys acting in their legal capacity and misconduct by others. This disciplinary system cannot help but have a detrimental effect on the public’s confidence in the Department’s ability to review misconduct by its own attorneys.

The OIG’s greatest asset is its highly dedicated personnel, so strategic management of human capital is paramount to achieving organizational performance goals. In this competitive job market, the OIG must make every effort to maintain and retain its talented workforce. The OIG’s focus on ensuring that its employees have the appropriate training and analytical and technological skills for the OIG’s mission will continue to bolster its reputation as a premier federal workplace, and improve retention and results. To that end, we are including a program increase in our budget request to modernize and strengthen our information technology program. We seek to expand our classified computing environment to keep up with the growing workload in that area; provide updated collaboration tools and web capabilities; procure a new case management system; and strengthen our IT support services. This modernization effort will allow the OIG to continue providing high quality, timely reports and reviews our stakeholders come to expect.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
IT Modernization	The IT modernization approach encompasses systems, applications, and personnel performing IT and cybersecurity processes, governance, and management and will improve mission effectiveness, create fiscal efficiencies and provide the right level of security to our systems and information. Areas targeted include classified computing, mission core applications, and IT services.	9	9	$5,260	32
Total		**9**	**9**	**$5,260**	

III. Appropriations Language and Analysis of Appropriations Language

The appropriation language states the following for the Office of the Inspector General:

For necessary expenses of the Office of Inspector General, $107,211,000, including not to exceed $10,000 to meet unforeseen emergencies of a confidential character: Provided, that not to exceed $4,000,000 shall remain available until September 30, 2022.

A. Analysis of Appropriations Language

No substantive changes proposed.

IV. Program Activity Justification

A. Audits, Inspections, Investigations and Reviews

OIG	Direct Pos.	Direct FTE	Amount
2019 Actual	476	451	$101,000
2020 Enacted	482	490	$115,000
Adjustments to Base and Technical Adjustments	0	-48	($13,049)
2021 Current Services	482	442	$101,951
2021 Program Increase	9	9	$5,260
2021 Request	491	451	$107,211
Total Change 2020-2021	9	-39	$2,211

OIG Information Technology Breakout	Direct Pos.	Direct FTE	Amount
2019 Actual	43.0	42.6	$13,108
2020 Enacted	48.0	47.6	$15,539
2021 Current Services	48.0	47.6	$16,306
2021 Program Increase	9.0	9.0	$5,260
2021 Request	57.0	56.6	$21,566
Total Change 2020-2021	9.0	9.0	$6,027

B. Program Description

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews.

C. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE (Goal 1)

Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.

WORKLOAD/RESOURCES	**FY2019**				**FY2020**				**FY2021**	
	Projected		**Actual**		**Projected**		**Actual as of 12-30-19**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	436	$97,250 [$13,728]	436	$101,000 [$14,120]	442	$105,000 [$14,669]	9	$2,211 [$382]	451	$107,211 [$15,051]
Performance Measure										
Number of Cases Opened per 1,000 DOJ employees:										
Fraud*		*		0.49		*		0.14		*
Bribery*		*		0.16		*		0.05		*
Rights Violations*		*		0.15		*		0.00		*
Sexual Crimes*		*		0.19		*		0.08		*
Official Misconduct*		*		1.05		*		0.20		*
Theft*		*		0.05		*		0.02		*
Workload										
Investigations closed ##		275		243		N/A		N/A		N/A
Integrity Briefings/Presentations to DOJ employees and other stakeholders		70		92		70		13		70
DOJ employees and stakeholders at Integrity Briefings		3,000		3,850		3,000		964		3,000

* Indicators for which the OIG only reports actuals.

## In FY20 this measure will no longer be used. The OIG's caseload has shifted to more complex and document-intensive cases (e.g., grant and contract fraud, leak matters) that require more in-depth financial and foresnsic analysis and document review. The OIG is also diversifying its caseload to extend more investigative coverage to other Department components. Therefore, this metric does not accurately reflect work load quality or cases closed.

PERFORMANCE AND RESOURCES TABLE (Goal 1)
(continued)

Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.

WORKLOAD/RESOURCES	**FY2019**				**FY2020**				**FY2021**	
	Projected		**Actual**		**Projected**		**Actual as of 12-30-19**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	436	$97,250 [$13,728]	436	$101,000 [$14,120]	442	$105,000 [$14,669]	9	$2,211 [$382]	451	$107,211 [$15,051]
Performance Measure										
Intermediate Outcome										
Percentage of BOP Investigations closed or referred for prosecution within 6 months of being opened [Refined Measure]		75%		86%		75%		97%		75%
Number of closed Investigations substantiated*		*		156		*		35		*
Arrests *		*		74		*		18		*
End Outcome										
Convictions *		*		64		*		12		*
Administrative Actions *				179				46		
Response to **Customer Surveys**:										
Report completed in a timely manner (%)		90%		100%		90%		100%		90%
Issues were sufficiently addressed (%)		90%		100%		90%		100%		90%

* Indicators for which the OIG only reports actuals.

PERFORMANCE AND RESOURCES TABLE (Goal 1)

Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.

Data Definition, Validation, Verification, and Limitations

A. Data Definition:

The OIG does not project targets and only reports actuals for workload measures, the number of closed investigations substantiated, arrests, convictions, and administrative actions. The number of convictions and administrative actions are not subsets of the number of closed investigations substantiated.

B. Data Sources, Validation, Verification, and Limitations:

Investigations Data Management System (IDMS) – consists of a web-based relational database system. It's a case management system.

The database administrator runs routine maintenance programs against the database. Database maintenance plans are in place to examine the internal physical structure of the database, backup the database and transaction logs, handle index tuning, manage database alerts, and repair the database if necessary. Currently, the general database backup is scheduled nightly and the transaction log is backed up in 3 hour intervals. We have upgraded to a web based technology.

Investigations Division Report of Investigation (ROI) Tracking System - a web-based SQL-Server application that tracks all aspects of the ROI lifecycle. The ROI and Abbreviated Report of Investigation (AROI) are the culmination of OIG investigations and are submitted to DOJ components. These reports are typically drafted by an agent and go through reviews at the Field Office and at Headquarters levels before final approval by Headquarters. The ROI Tracking System reads data from IDMS. By providing up-to-the-minute ROI status information, the Tracking System is a key tool in improving the timeliness of the Division's reports. The ROI Tracking System also documents the administration of customer satisfaction questionnaires sent with each completed investigative report to components and includes all historical data. The system captures descriptive information as well as questionnaire responses. Descriptive information includes the questionnaire form administered, distribution and receipt dates, and component and responding official. The database records responses to several open-ended questions seeking more information on deficiencies noted by respondents and whether a case was referred for administrative action and its outcome. Questionnaire responses are returned to Investigations Headquarters and are manually entered into the Tracking System by Headquarters personnel. No data validation tools, such as double key entry, are used though responses are entered through a custom form in an effort to ease input and reduce errors.

Investigations Division Investigative Activity Report – Most of the data for this report is collected in IDMS. The use of certain investigative techniques and integrity briefing activities are also tracked externally by appropriate Headquarters staff.

C. FY 2019 Performance Report:

The workload measure "Investigations Closed" will no longer be tracked starting in FY20. The OIG is focusing on more complex and document-intensive cases (e.g., grant and contract fraud) that require more in-depth financial and forensic analysis.

PERFORMANCE MEASURE TABLE (Goal 1)

Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.

Performance Measure Report Workload	FY2015	FY2016	FY2017	FY2018	FY2019		FY2020		FY2021	FY2022
	Actuals	Actuals	Actuals	Actuals	Projected	Actual	Projected	Actuals through 12/30/19	Projected	Projected
Number of Cases Opened per 1,000 DOJ employees:										
Fraud*	0.47	0.42	0.55	0.58	*	0.49	*	0.14	*	*
Bribery*	0.10		0.09	0.13	*	0.16	*	0.05	*	*
Rights Violations*	0.12	0.14	0.15	0.18	*	0.15	*	0.00	*	*
Sexual Crimes*	0.39	0.21	0.25	0.25	*	0.19	*	0.08	*	*
Official Misconduct*	1.19	1.17	1.18	1.04	*	1.05	*	0.20	*	*
Theft*	0.17	0.11	0.11	0.1	*	0.05	*	0.02	*	*
Investigations closed ##	357	312	308	255	275	243	N/A	N/A	N/A	N/A
Integrity Briefings and Presentations to DOJ employees and other stakeholders	82	83	83	90	70	92	70	13	70	70
DOJ employees and stakeholders attending Integrity Briefings	3,975	3,799	5,419	4,606	3,000	3,850	3,000	964	3,000	3,000
Intermediate Outcome										
Percentage of **BOP** Investigations closed or referred for prosecution within 6 months**	76%	83%	92%	87%	75	86%	75	97%	75	*
Number of closed Investigations substantiated (QSR Measure)*	226	196	204	161	*	156	*	35	*	*
Arrests*	96	91	116	94	*	74	*	18	*	*
End Outcome										
Convictions*	73	88	84	60	*	64	*	12	*	*
Administrative Actions	225	251	219	252	*	179	*	46	*	*
Response to Customer Surveys:										
Report completed in a timely manner (%)	90%	98%	93%	90%	90%	100%	90%	100%	90%	90%
Issues were sufficiently addressed (%)	90%	98%	98%	90%	90%	100%	90%	100%	90%	90%

* Indicators for which the OIG only reports actuals.

## Beginning in FY20, the measure will no longer be tracked.

PERFORMANCE AND RESOURCES TABLE (Goal 2)										
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews										
DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.										
OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.										
WORKLOAD/RESOURCES	**FY2019**				**FY2020**				**FY2021**	
	Projected		**Actual**		**Projected**		**Actual as of 12/30/19**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(Reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total.)	436	$97,250 [$13,728]	436	$101,000 [$14,120]	442	$105,000 [$14,669]	9	$2,211 [$382]	451	$107,211 [$15,051]
Performance Measure										
Workload										
Audit and E&I assignments initiated		87		98		87		16		87
Percent of CSITAO* resources devoted to security reviews of major DOJ information systems		80%		94%		80%		92%		80%
Percent of internal DOJ audit reports that assess component performance measures		25%		73%		30%		71%		40%
Percentage of E&I assignments opened and initiated during the fiscal year devoted to Top Management Challenges		70%		75%		70%		75%		70%
Percent of direct resources devoted to audit products related to Top Management Challenges, and GAO and JMD-identified High-Risk Areas		85%		96%		85%		94%		85%
Intermediate Outcome										
Audit and E&I assignments completed		87		114		87		13		87
*Computer Security & Information Technology Audit Office										

PERFORMANCE AND RESOURCES TABLE (Goal 2)
(continued)

Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.

WORKLOAD/RESOURCES	**FY2019**				**FY2020**				**FY2021**	
	Projected		**Actual**		**Projected**		**Actual as of 12/30/19**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	436	$97,250 [$13,728]	436	$101,000 [$14,120]	442	$105,000 [$14,669]	9	$2,211 [$382]	451	$107,211 [$15,051]
Performance Measure										
Intermediate Outcome										
Percent of Audit resources devoted to reviews of contracts and contract management		10%		12%		8%		11%		8%
Components receiving information system audits		6		10		6		6		6
Number of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I. #		N/A		N/A		N/A		12		
Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I		90%		96%		90%		100%		90%
Percent of internal DOJ (E&I) reviews to be provided to the IG as a working draft within an average of 12 months***		35%		40%		35%		N/A		35%
Percent of grant, CODIS, equitable sharing, and other external audits to be completed in draft within 8 months		40%		59%		40%		100%		40%
Percent of less complex internal DOJ audits to be provided to the IG as a working draft within 8 months. ##		50%		100%		N/A		N/A		N/A
Percent of internal DOJ audits to be provided to the IG as a working draft within 13 months		50%		90%		50%		86%		50%

*** This measure was refined in FY 2019 to reflect all reviews with a deadline of 12 months.

# New Line item to assist Audit and E&I in separating their data for more accuracy

## This measure will no longer be used. We will refine our measure beginning in FY 2020 on "more complex" DOJ internal audits to reflect all internal DOJ audit reports with a deadline of 13 months.

PERFORMANCE AND RESOURCES TABLE (Goal 2) (continued)

Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.

Data Definition, Validation, Verification, and Limitations

A. Data Definition:

"Assignment" covers all audits (including internals, CFO Act, and externals, but **not** Single Audits), evaluations, and inspections. "Assignments" may also include activities that do not result in a report or product (e.g., a memorandum to file rather than a report); or reviews initiated and then cancelled.

B. Data Sources, Validation, Verification, and Limitations:

Project Resolution and Tracking (PRT) system- PRT was implemented on April 18, 2011; this OIG system was designed to track audits, evaluations, and reviews from initiation to completion, including the status of recommendations. The system provides senior management with the data to respond to information requests and track and report on current status of work activities.

C. FY 2019 Performance Report: N/A

PERFORMANCE MEASURE TABLE (Goal 2)

Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the Rule of Law and Integrity in the proper administration of Justice.

OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.

Performance Measure Report	FY2015	FY2016	FY2017	FY2018	FY2019		FY2020		FY2021	FY2022
	Actuals	Actuals	Actuals	Actuals	Projected	Actual	Projected	Actual as of 12/30/19		Projected
Workload										
Audit and E&I assignments initiated	106	109	104	97	87	98	87	16	87	87
Percent of CSITAO resources devoted to security reviews of major DOJ information systems	88%	97%	97%	91%	80%	94%	80%	92%	80%	80%
Percent of issued internal DOJ audit reports that assess component performance measures	42%	67%	72%	91%	25%	73%	30%	71%	40%	40%
Percentage of E&I assignments opened and initiated during the fiscal year devoted to Top Management Challenges.	80%	86%	100%	66%	70%	75%	70%	75%	70%	70%
Percent of direct resources devoted to audit products related to Top Management Challenges, and GAO and JMD-identified High-Risk Areas	96%	95%	92%	88%	85%	96%	85%	94%	85%	85%
Intermediate Outcome										
Audit and E&I Assignments completed	109	98	112	96	87	109	87	13	87	87
Percent of Audit resources devoted to reviews of contracts and contract management	13%	14%	14%	16%	10%	12%	8%	11%	8%	8%
Components receiving information system audits	8	9	10	10	6	10	6	6	6	6
Number of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I #	N/A	N/A	N/A	N/A	N/A	N/A	N/A	12	N/A	N/A
Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I	100%	100%	92%	96%	90%	96%	90%	100%	90%	90%
Percent of internal DOJ (E&I) reviews to be provided to the IG as a working draft within an average of 12 months ***	N/A	N/A	N/A	N/A	35%	40%	35%		35%	35%
Percent of grant, CODIS, equitable sharing, and other external audits to be completed in draft within 8 months	58%	50%	50%	51%	40%	59%	40%	100%	40%	40%
Percent of less complex internal DOJ audits to be provided to the IG as a working draft within 8 months ##	40%	100%	100%	100%	50%	100%	N/A	N/A	N/A	N/A
Percent of internal DOJ audits to be provided to the IG as a working draft within 13 months	83%	73%	83%	88%	50%	90%	50%	86%	50%	50%

*** This measure will be refined in FY 2019 to reflect all reviews with a deadline of 12 months.

# New Line item to assist Audit and E&I in separating their data for moer accuracy

## This measure will no longer be used. We will refine our measure; beginning in FY 2020 on "more complex" DOJ internal audits to reflect all internal DOJ audit reports with a deadline of 13 months.

V. Performance, Resources, and Strategies

1. Performance Plan and Report for Outcomes

As illustrated in the preceding Performance and Resources Tables, the OIG helps the Department achieve its strategic goals and promotes efficiency, integrity, economy, and effectiveness through its audits, inspections, investigations, and reviews. For the Department's programs and activities to be effective, Department personnel, contractors, and grantees must conduct themselves in accordance with the highest standards of integrity, accountability, and efficiency. The OIG investigates alleged violations of criminal and civil laws, regulations, and ethical standards arising from the conduct of the Department's employees in their numerous and diverse activities.

The OIG continues to review its performance measures and targets, especially in light of the changing nature of the cases it investigates and the Department programs it audits and reviews. Today's work is much more complex and expansive than it was only a few years ago. The number of documents to be reviewed, the number of people to interview, the amount of data to examine, and the analytical work involved in many OIG products are significantly greater than in prior years. The OIG ensures sufficient time and resources are devoted to produce high-quality, well-respected work.

2. Strategies to Accomplish Outcomes

The OIG will devote all resources necessary to investigate allegations of bribery, fraud, abuse, civil rights violations, and violations of other laws and procedures that govern Department employees, contractors, and grantees, and will develop cases for criminal prosecution and civil and administrative action. The OIG will continue to use its audit, inspection, evaluation, and attorney resources to review Department programs or activities identified as high-priority areas in the Department's Strategic Plan, and focus its resources to review the Department's Top Management and Performance Challenges.

VI. Program Increases by Item

Item Name: Information Technology (IT) Modernization/Infrastructure

Strategic Goal(s) & Objective(s): Uphold the Rule of Law and Integrity in the proper administration of Justice.
Organizational Program: Office of the Inspector General (OIG)

Program Increase: Positions 9 Agt/Atty/Other 0/0/9 FTE 9 PersonDollars $1,760,000
Equipment/software/services: Dollars $3,500,000

Total Request of Increase: $5,260,000

1. Description of Item

To meet the OIG's evolving operational and mission needs, the OIG requests a program increase of $5,260,000 to modernize its information technology (IT) infrastructure. Specifically, in recent years, the OIG's mission has evolved to require a greater need for collaboration and information sharing, digital forensics, data analytics, and increased IT security—all of which require an increased investment in the OIG's IT infrastructure. Some of our legacy IT systems are reaching the end of their useful life, and we do not have sufficient IT personnel with the skills necessary to build and maintain the IT infrastructure at its current level.

As a result, the OIG created its new Information Technology Division (ITD), so that the OIG could better focus on ensuring that it has the IT capabilities it needs to execute its mission. To that end, ITD's first task was to do an assessment of the OIG's current IT personnel and infrastructure and to determine whether it was sufficient to the meet the OIG's current and future IT needs. As a result of this assessment, ITD is executing an IT modernization approach focused towards driving IT consolidation and efficiencies, improving the acquisition of resources, improving security postures, and maintaining a common IT strategy to allow the OIG's Audit, Evaluation and Inspections, Investigations, and Oversight and Review Divisions to focus on their core oversight missions. The approach takes into account the various OIG Divisions' business and mission strategies and is designed to enhance and enable those strategies. The IT modernization approach encompasses systems, applications, and personnel performing IT and cybersecurity processes, governance, and management.

Transforming the OIG IT systems and processes into a modern, flexible architecture that maximizes the use of limited resources will be a multi-year effort requiring close coordination among the OIG Divisions and the DOJ Office of the Chief Information Officer. This transformation requires new levels of transparency into IT activities and costs so that decision-making processes will lead to informed choices that enable the workforce of the future.
IT modernization will allow the OIG to execute its mission more efficiently and effectively and to provide the right level of security for its IT systems and information. Consolidation and standardization allows centralized acquisitions to take full advantage of economies of scale. Security posture is enhanced through improved and more controlled assessments of the network architecture and the resources accessing the network. In addition, an enterprise-wide implementation strategy ensures there are no gaps in engineering, budgeting, service delivery, or resource management. The modernization approach will take advantage of ongoing efforts and

leverage existing IT governance, policies, and processes and will ultimately enable a necessary shift in the infrastructure used to support employees and mission support operations.

2. Justification

In recent years, advances in technology have forced the OIG to rethink both how it operates internally and how it executes its mission. For example, the OIG is increasing its oversight of the Department's national security activities, which will require the OIG to enhance its ability to acquire, maintain, and analyze large quantities of classified data in a secure manner. In addition, many of the OIG's core mission applications are either reaching the end of their useful life or do not have the capabilities necessary to fulfill OIG mission needs. Further, the OIG does not have the IT personnel necessary to maintain, secure, and further develop the OIG's IT systems and core mission applications, which requires the OIG to be overly reliant on the availability of contractors to meet its mission goals.

The requested program increase targets the fulfillment of the OIG core missions in parallel with ITD's modernization goals and enterprise strategies. Currently, OIG Divisions are modernizing and improving the effectiveness and efficiency of their own IT operations. However, these Division-specific activities will not lead to an enhanced IT management and operational environment on an enterprise level. Accordingly, the OIG requests the specific program enhancements described below to support its IT modernization initiative.

Classified Computing

In recent years, the Department has identified enhancing national security and countering the threat of terrorism as one of its top strategic goals. Accordingly, the OIG has increased its national security-related oversight activities, both as a recognition of the importance of the Department's national security mission and of the inherent and significant risks that are associated with fraud, waste, abuse, mismanagement and misconduct as it relates to the Department's activities in this area. For example, the OIG has recently completed reports related to the FBI's polygraph and insider threat programs. The OIG is currently reviewing the FBI's covert contracts and national security undercover operations. In addition, the Department, the Congress, and the public have increasingly requested that the OIG initiate national security related security reviews to address concerns relating to sensitive and high-profile matters, such as our recent review of the Department's and the FBI's compliance with legal requirements and policies in applications filed with the U.S. Foreign Intelligence Surveillance Court relating to a certain U.S. person.

With a growing amount of highly-classified, national security work, the OIG needs to expand Secret and Top Secret capabilities, build Sensitive Compartmented Information Facilities (SCIFs), and add new secure phones in field offices. This will expand the OIG's ability to perform national security oversight in support of the OIG mission. Further, this will allow the OIG to move away from using classified laptops, which increases the risk of the loss of equipment and classified data, and become fully compliant with DOJ classified information policies and processing requirements.

The OIG is requesting **$1.5 million** to expand infrastructure for handling and storing classified information.

Core Mission Applications

Case Management Systems

The OIG currently has two highly critical systems reaching end of life: one that tracks investigative cases to record, retrieve, and deliver information necessary for the execution and management of complaints and allegations about Department employees, contractors, and grantees; and one for audits, which is used to plan, conduct, and document audit work, and to capture audit findings. For both of these systems, the vendor will cease support within the next one to four years, meaning the OIG will not receive patches or technical support for outages or other issues, creating a significant risk to business operations. In addition, the OIG's Investigations and Audit Divisions are looking to expand capabilities, such as mobility, collaboration, and cloud accessibility, as well as develop better methods for fulfilling complex legal discovery and government archiving requirements.

The OIG is requesting **$2 million** for mission-critical case management systems supporting OIG audits and investigations.

Electronic Discovery (eDiscovery)

The OIG is requesting dedicated funding that will permit it to establish an OIG-wide, enterprise eDiscovery capability using Relativity. The OIG has increasingly used Relativity as its eDiscovery tool of choice, which provides powerful data mining capabilities. Currently, the OIG uses several different tools for data mining and analysis, and this investment will allow the OIG to use one tool across the entire OIG.

At present, the OIG has funded two eDiscovery contractors using base funds taken from other program areas, who are mainly focused on ongoing support to eDiscovery case work occurring in only two OIG Divisions.

The OIG is requesting **$696,000** for three (3) permanent, full-time positions to replace the contractors. The employees would continue to support case work, but would also be available to work on future enterprise capabilities for the entire OIG.

SharePoint

The OIG is expanding its collaborative platforms and uses SharePoint as a central tool for this purpose. Our recent upgrade provided many functions that require additional IT support to maintain and develop services for employees.

Therefore, the OIG is requesting **$167,000** for one (1) additional permanent, full-time IT support position for SharePoint.

IT Services

IT Security

The OIG is requesting **$398,000** for two (2) permanent, full-time positions to ensure a safe network security posture where network protection and intrusion prevention are paramount to the OIG's cybersecurity goals. The additional personnel will help certify that cybersecurity policies are applied and adhered to, including continued testing and scrutiny of network traffic.

Help Desk
The OIG is requesting $**500,000** for three (3) permanent, full-time positions, which would establish an IT support presence in major OIG field sites to provide more direct, local customer support.

3. Current State and Impact on Performance

Without the requested funding, the OIG will be forced to redirect funds that would normally be used for our audits, reviews, investigations, and other oversight functions to maintaining its IT infrastructure. Currently, the OIG ITD provisions voice, video, data, and application hosting and housing services to the OIG employees and its direct support contractors. ITD also provides desktop and worker productivity solutions, including mobile devices and cellular voice/data service. Additionally, ITD provides acquisition and enterprise license support for customers requiring hardware, software, and support services.

The enhancement request will contribute to the alignment of structure, process, and people to transition the vast majority of commodity IT. This model will enable ITD and its staff to focus on policy, governance, architecture, and standards and the provisioning of core infrastructure and commodity IT through managed services, leveraging commercial providers where possible, to meet mission outcome and security requirements.

A commitment to a unified approach to IT modernization will deliver foundational improvements in the enterprise that will enable shared services, improve the speed and flexibility of operations, and create a more agile virtual workforce for the 21st century.

Funding
IT Modernization
(Dollars in Thousands)

Base Funding

FY 2019 Actual				FY 2020 Enacted				FY 2021 Current Services			
Pos	Agt/Atty	FTE	$0	Pos	Agt/Atty	FTE	$0	Pos	Agt/Atty	FTE	$0
26	0/0	25.6	$9,825.0	31	0/0	30.6	$10,387.0	31	0/0	30.6	$10,491.0

Personnel Increase Cost Summary

Type of Position	Modular Cost per Position ($000)	1st Year Annualization	Number of FTEs Requested	FY 2021 Requested ($000)	FY 2022 Annualization (change from 2020) ($000)	FY 2023 Annualization (change from 2021) ($000)
IT Specialists	$232.4	$232.4	4	$929.6	($43.2)	$28.0
IT Specialists	$166.5	$166.5	5	$832.5	($59.5)	$25.0
Total Personnel			9	$1,762.1	($102.7)	$53.0

Total Request for this Item

	POS	Agt/Atty /Other	FTE	Personnel ($000)	Non-personnel ($000)	Total ($000)	FY 2022 Annualization (change from 2020) ($000)	FY 2023 Annualization (change from 2021) ($000)
Current Services	31	0/0/31	30.6	$ 6,753.0	$ 3,738.0	$ 10,491.0		
Increases	9	0/0/9	9	$ 1,760.0	$ 3,500.0	$ 5,260.0	$ (102.7)	$ 53.0
Grand Total	40	0/0/40	39.6	$ 8,513.0	$ 7,238.0	$ 15,751.0	$ (102.7)	$ 53.0

VII. Program Offsets by Item

The Office of the Inspector General has no program offsets to submit in the FY 2021 budget request.

APPENDIX

Statistical Highlights

April 1, 2019 – September 30, 2019

The following table summarizes the OIG activities discussed in our most recent *Semiannual Report to Congress.* As these statistics and the following highlights illustrate, the OIG continues to conduct wide-ranging oversight of Department programs and operations.

April 1, 2019 - September 30, 2019	
Allegations Received by the Investigations Division	6,195
Investigations Opened	127
Investigations Closed	125
Arrests	42
Indictments/Information	32
Convictions/Pleas	40
Administrative Actions	87
Monetary Recoveries	$ 917,501
Audit Reports Issued	41
Questioned Costs	$4,577,633
Funds for Better Use	$1,048,000
Recommendations for Management Improvements	270
Single Audit Act Reports Issued	30
Questioned Costs	$12,682,652
Recommendations for Management Improvements	77
Other Audit Division Reports Issued	2

EXHIBITS